ext4: fix use-after-free in update_super_work when racing with umount

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-31446
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:38 UTC
Updated	2026-05-07 19:21:44 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ext4: fix use-after-free in update_super_work when racing

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.000240000 probability, percentile 0.067850000 (date 2026-04-27)

Problem Types: CWE-416

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 52c3a04f9ec2a16a4204d6274db338cb8d5b2d74 c8fe17a1b308c3d8c703ebfb049b325f844342c3 git
CNA	Linux	Linux	affected b98535d091795a79336f520b0708457aacf55c67 c4d829737329f2290dd41e290b7d75effdb2a7ff git
CNA	Linux	Linux	affected b98535d091795a79336f520b0708457aacf55c67 9449f99ba04f5dd1c8423ad8a90b3651d7240d1d git
CNA	Linux	Linux	affected b98535d091795a79336f520b0708457aacf55c67 034053378dd81837fd6c7a43b37ee2e58d4f0b4e git
CNA	Linux	Linux	affected b98535d091795a79336f520b0708457aacf55c67 c97e282f7bfd0c3554c63d289964a5ca6a1d2ffe git
CNA	Linux	Linux	affected b98535d091795a79336f520b0708457aacf55c67 08b10e6f37fc533a759e9833af0692242e8b3f93 git
CNA	Linux	Linux	affected b98535d091795a79336f520b0708457aacf55c67 d15e4b0a418537aafa56b2cb80d44add83e83697 gi
CNA	Linux	Linux	affected 585ef03c9e79672781f954daae730dfe24bf3a46 git
CNA	Linux	Linux	affected afe490e48d47df1b3f64012835c1bc2f075a8c8b git
CNA	Linux	Linux	affected 5.18
CNA	Linux	Linux	unaffected 5.18 semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.131 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/034053378dd81837fd6c7a43b37ee2e58d4f0b4e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/08b10e6f37fc533a759e9833af0692242e8b3f93	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c8fe17a1b308c3d8c703ebfb049b325f844342c3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch

git.kernel.org/stable/c/c4d829737329f2290dd41e290b7d75effdb2a7ff	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9449f99ba04f5dd1c8423ad8a90b3651d7240d1d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/d15e4b0a418537aafa56b2cb80d44add83e83697	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c97e282f7bfd0c3554c63d289964a5ca6a1d2ffe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.